(19) Europäisches Patentamt
Eur pean Patent Offic
Office europ´en des brevets

(11) Publication number: **0 417 447 A2**

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **90114545.8**

(51) Int. Cl.5: **G06F 1/00**

(22) Date of filing: **28.07.90**

(30) Priority: **12.09.89 US 405910**

(43) Date of publication of application:
20.03.91 Bulletin 91/12

(84) Designated Contracting States:
DE FR GB IT

(71) Applicant: **International Business Machines Corporation**
Old Orchard Road
Armonk, N.Y. 10504(US)

(72) Inventor: **Double, Glen Paul**
8834 High Ridge Lane
Concord, North Carolina 28025(US)
Inventor: **Weingart, Steve Harris**
11 Fox Hill Road
Peekskill, New York 10566(US)

(74) Representative: **Herzog, Friedrich Joachim, Dipl.-Ing.**
IBM Deutschland GmbH Schönaicher Strasse 220
W-7030 Böblingen(DE)

(54) Data protection by detection of intrusion into electronic assemblies.

(57) The present invention provides an intrusion barrier for protecting against mechanical or chemical intrusion into an electronic assembly, especially one containing volatile memory. It includes a screen material surrounding the electronic assembly which screen material has formed thereon fine conductive lines in close proximity to each other. The lines are formed of conductive particles of material dispersed in a solidified matrix of a material which looses its mechanical integrity when removed from the screen. An electrical supply and signal detection circuit is provided which generates an output signal responsive to a given change in resistance of the conductive lines, such that if the resistance changes are a result of a mechanical or chemical attack, a signal is generated which can cause the erasure of the volatile memory. Also, preferably radiation detection and temperature sensing circuits are provided to cause erasure of the volatile memory responsive to detection of a given intensity of radiation or a temperature below a given value.

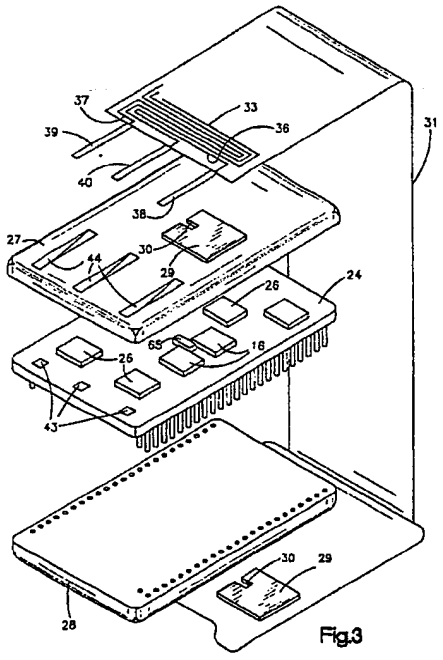

Fig.3

EP 0 417 447 A2

DATA PROTECTION BY DETECTION OF INTRUSION INTO ELECTRONIC ASSEMBLIES

Field of the Invention

This invention relates generally to detection of intrusion into electronic assemblies, and more particularly, to the detection of intrusion by mechanical or chemical means for the purpose of reading the data stored in a memory.

In many computer applications, it is desirable to protect the contents of the computer memory from being unlawfully or unauthorizedly extracted and read. It is conventional practice to prevent reading of information electronically by providing certain encryption schemes wherein data is transmitted and received in an encrypted form and only authorized people who have the decryption key are able to read the data. There are many different types of encryption schemes which are useful in protecting the sensitive data against being read by unauthorized persons. Encryption keys and other sensitive data are often stored in I/C (integrated circuit) memory components within the computer. By use of software, the stored information is generally adequately protected from unauthorized persons using keyboard entries to attempt memory interrogation. However, an unauthorized person with the necessary skills and knowledge, and sufficiently motivated can bypass software controls and attack the computer hardware directly. There are many attacks some straight forward and well known, others more sophisticated, that allow direct interrogation of memory components and devices. One scheme of protection against such attacks is to provide some type of detecting means which detect any attempted mechanical intrusion into the sensitive area of the computer and, when such intrusion is detected an alarm is given and/or a signal is sent to circuitry, which circuit erases the data, thereby preventing the compromise of the information which was stored in the computer memory components. Various schemes have been proposed which provide for some type of electronic or electrical grid surrounding the computer circuitry and, when this electrical grid is broken or breached, the requisite signal is generated. Schemes for such electronic detection are shown in U.S. Patents 4,446,475 and 3,594,770. These types of systems, however, have several drawbacks. One such drawback is that many grids are susceptible to very careful mechanical manipulation to allow the memory device to be accessed without breaking or otherwise compromising the circuit. Also, certain of these systems are susceptible to a type of attack wherein the materials which support the electrical grid are chemically attacked leaving access areas exposed to circumvent the electrical grid thus allowing physical intrusion into the memory components.

Still other more sophisticated attacks, through temperature modification or though ionizing radiation (e.g. x-rays) affect volatile memory devices such that an erasure command is not effective, thereby allowing the electrical wrapping to be circumvented.

The present invention overcomes these defects by providing an outer intrusion detection layer that is highly resistant to chemical and mechanical attacks. Further, internal circuitry is provided to detect temperature and ionizing radiation attacks.

Use of detection for low temperatures to prevent tampering is shown in U.S. Patent 4,593,384. Also, temperature responsive devices for safeguarding information are shown in U.S. Patent 3,851,602. The use of means to limit effects of ionizing radiation are shown in U.S. Patents 4, 413,327 and 4,639,826. However, neither of these patents suggest any means of security protection and/or erasing of information responsive to very high levels of radiation applied for purpose of attacking a volatile memory device to obtain sensitive information.

Summary of the Invention

According to one aspect of the present invention, an intrusion barrier for protecting against mechanical or chemical intrusion into an electronic assembly is provided. The barrier includes a screen material surrounding the electronic assembly. The screen material has formed thereon fine conductive lines in close proximity to each other in a pattern that limits the mechanical access which can be achieved without disturbing the resistive characteristics of at least one line or line segment. The lines are formed of conductive particles of material dispersed in a solidified matrix of material which loses its mechanical integrity when removed from the screen substrate. Electrical supply and signal detection means are provided which are adapted to supply a signal to the conductive lines and generate an output signal responsive to a given change in the resistance of the conductive lines whereby, when the resistance of the conductive lines changes, either as result of chemical attack or mechanical attack, a signal is generated. This signal can be made to cause the erasure of information in the memory component. In other aspects of the present invention, radiation d tection means are provided which generate a signal when

radiation is detected above a given intensity and which signal is utilized to cause the erasure of information contained in the memory component before the radiation has reached a level adequate over a reasonable period of time to prevent erasure. In still further aspects, the invention includes temperature sensing means which generates an electrical signal responsive to a temperature which is lower than a predetermined value and which signal is used to cause the erasure of information contained in the memory component, before the temperature of the memory component has reached a temperature low enough to cause a significant number of its storage locations to retain their information even after erasure is attempted.

Description of the Drawings

Fig. 1 is a schematic view of a message encryption/decryption system;

Fig. 2 is a schematic view of the operation of the encryption/decryption system and means to detect and prevent unauthorized interrogation of the system;

Fig. 3 is an exploded perspective view of a circuit card with various devices and components mounted thereon which constitute the system to be protected, and, showing plastic preforms which mate with the card to provide the form-factor for wrapping the flexible screen membrane;

Fig. 4 is a perspective view, somewhat diagrammatic showing a flexible screen member used in this invention;

Fig. 5 is the system of Fig. 3 showing the flexible screen member partially wrapped thereon with screen leads attached to the circuit card;

Fig. 6 is a sectional view taken substantially along the plane of line 6-6 of Fig. 5;

Fig. 7 is a view similar to Fig. 5 in which the screen is wrapped onto the circuit card with parts broken away for clarity;

Fig. 8 is a view similar to Fig. 6 showing the assembly encapsulated in epoxy and contained in a steel container;

Fig. 9 is a sectional view taken substantially along the plane of line 9-9 of Fig. 8;

Fig. 10 is a circuit diagram of a circuit used for detecting mechanical or chemical intrusion through the screen member;

Fig. 11 is a circuit diagram of the circuit used for detecting and obtaining of data by use of high intensity radiation; and

Fig. 12 is a circuit diagram of the circuit used for detecting and preventing obtaining of information by low temperature excursions.

Description of an Embodiment

Referring now to the drawings and for the present to Fig. 1, a conceptual schematic drawing of a message encryption\decryption facility is shown in broken outline 10. The clear message which is to be encrypted is delivered to encryption means 12 which in turn encrypts the clear message via key store 14 to provide an encrypted message. The encryption keys in key store 14 as well as the encryption 12 must be protected from interrogation because if an unauthorized person were to have access to these keys and the encryption process, the clear messages could be derived from encrypted data and misused indiscriminately.

The conceptual block diagram in Fig. 2 shows the scheme of the present invention for detecting and preventing unauthorized interrogation of the stored encryption keys in key store 14. For the purpose of this invention, the encryption keys are retained in a volatile memory 16. The volatile memory 16 is powered by either a battery or system power determined by power switch 18. Power to the memory is controlled by power gate 20 and shorting transistor 21 via detection logic NAND gate 22 which in turn is actuated by sensor circuits designated S, T and X. (Of course, more sensor inputs could be used if desired.) Sensor circuit S, which will be described presently in detail, detects mechanical or chemical intrusion; sensor circuit T, which will be described presently in detail, detects temperature excursions; and sensor circuit X, which will be described presently in detail, detects exposure to radiation. As is well known in the art, the logic NAND gate 22 will normally be in the "low" or "off" condition if all inputs are "on" or "high"; however, if any input goes "low", then the NAND gate output 22 goes "high" providing a signal to other components attached to it. Such a signal from the NAND gate output will cause the power gate 20 to disconnect the memory 16 from power and cause shorting transistor 21 to short the power pin of the memory to ground thus erasing the memory quickly. Thus, if any one of the sensor inputs changes from "high" to "low", as a result of certain predetermined conditions indicating an attack the NAND gate 22 will turn "on" and the data from memory 16 will be quickly erased. Each of these particular detecting circuits will be described presently.

As shown in Fig. 3, a circuit card 24 is provided which contains thereon the various components for encryption, key storage in volatile memory 16, the battery and the protection circuitry for the volatile memory for the encryption/decryption facility 10. The components other than the volatile memory 16 are designated generally as 26, all

being shown conceptually. These components also include a battery. The specific location, number and function are not critical to this invention.

Disposed over each side of the circuit card 24 are a pair of plastic preforms 27 and 28 which fit over the components and provide the proper control surface or form-factor for the wrapping of the screen member which will be described presently. If the circuit card 24 employs pins, then holes (unnumbered) or slots to receive such pins are provided in preform 28. Patterned Lead foil sheets 29 are placed on the plastic preforms 27 and 28 so as to provide a radiation shield on both side of the volatile memory storage components 16. The foil sheets 29 have cut out portions 30 to accommodate the positioning of a radiation sensor as will be described presently. The circuit card 24, the preforms 27 and 28 and the Lead sheets 29 are all stacked in superimposed relationship so as to receive a screen member 31 (Figs. 3 through 6) wrapped there around which will form the barrier against any unauthorized attempts at mechanical or chemical intrusion to the circuit card 24.

As seen in Figs. 4 through 6, the screen member 31 is comprised of a tough flexible substrate such as film 32 of Mylar (a trade mark of E. I. DuPont Co. for polyethylene terepthalate) having a serpentine pattern of screened conductive lines 33 thereon. The lines 33 are comprised of conductive particles 34 such as particles of silver and carbon which are dispersed in an organic matrix material such as polyvinyl chloride. These lines 33 are screened onto the Mylar film by conventional screening processes and are sufficiently close together and of a size to provide a deterrent to mechanical probing of the circuit card. A preferred geometry comprises lines .25 mm wide and .013 mm thick and spaced on about .5 mm centers. A thin acrylic film 35 (Fig. 6) over the lines 33 provides environmental protection to the lines, from such things as moisture and atmospheric contaminants. Referring to Fig. 4, the lines 33 are screened onto the substrate 32 by conventional silk screening techniques in a serpentine pattern such that they form two legs or segments 36 and 37 of substantially equal resistance, one leg 36 terminating in an electrical contact 38 and the other leg 37 terminating in an electrical contact 39, both legs 36 and 37 having a common center electrical contact 40. Two legs 36 and 37 will act as two resistance legs in a bridge circuit, which will be described presently.

The screen is formed with a pair of side flaps 41 which serve to protect the edges of the circuit card as will be described presently.

The substrate 31 is also preferably provided with an adhesive backing 42, and as shown in Fig. 5, the screen member 31 is partially wrapped around the superimposed circuit card, plastic preforms and lead strips. The electrical contacts 38, 39 and 40 are connected to their respective terminals 43 on the circuit card 24 through openings 44 in the preform 27. These terminals 43 are mainly schematic or conceptual representations of the contact points on the card 24 to connect to the circuit shown in Fig. 10. The remaining portion of the screen membrane is then wrapped around completely to cover the screen contacts and the side flaps 41 are folded over the preform sides as shown in Fig. 7. This configuration provides a card with components thereon which is essentially completely enclosed with a screen that has conductive line formed thereon with the adhesive 42 providing a bond to the preforms 27 and 28. The assembly shown in Fig. 7 is then placed in a steel container 45 and completely encapsulated with a thin layer of epoxy 46 which becomes very hard and brittle upon curing as shown in Figs. 8 and 9. The container 45 provides a degree of EMI shielding for the circuit card 24 components. The epoxy 46 is chosen such that it is harder and more brittle, and more rugged and durable than the materials making up the screen number. Attempts to mechanically remove the epoxy 46 will result in a variety of fracture modes which will in turn cause lines 33 to break or rupture when the epoxy fractures. The bonding of the epoxy 46 to the screen is of a type such that it is extremely difficult to separate the epoxy mechanically from the screen without disrupting the underlying lines 33. Further, the strength of the bond of the epoxy 46 to the lines 33 is stronger than the strength of the bond of the lines 33 to the substrate 32 and thus will thwart any attempted mechanical intrusion through the epoxy 46 and screen 31 to get to the volatile memory components 25. The epoxy material 46 is chosen such that the epoxy and the materials making up the screen number 31 are both subject to attack by similar solvents or reagents, and thus attempts to dissolve the epoxy 46 are highly likely to result in chemical attack of the lines 33 by the solvent which will cause changes in resistance which may even become either shorts, or opens in the lines 33.

The contacts 38, 39 and 40 are attached to a circuit for the Sensor S through terminals 44 on the card 24 as shown in the circuit diagram of Fig. 10. The circuit includes resistor 54, 55 and 56 connected in series, and a pair of operational amplifiers 57 and 58. The negative input of operational amplifier 57 and positive input of operational amplifier 58 are connected to the center contact 40 of the lines 33. Contact 38 of line 33 is connected to system power or battery via power switch 18 and contact 39 of line 33 is connected to ground. The resistors 54, 55, and 56 are connected in series

between system power or battery and ground. Resistors 54 and 56 are chosen to be of equal value. The value chosen for resistor 55 in relationship to the value of resistors 54 and 56 provides upper and lower bounds on the resistance differences between the legs 36 and 37 of the screen. The positive input of operational amplifier 57 is connected between resistors 54 and 55 and the negative input of amplifier 58 is connected between resistors 55 and 56. In this configuration, when the resistance of legs 36 and 37 of lines 32 are equal, both amplifiers 57 and 58 will be turned on. However, if the resistance of either leg 36 or 37 is substantially increased or decreased beyond the bounds set by resistor 55, the bias of the operation amplifiers 57 and 58 will change such that one or the other will turn "off" thus changing the input to NAND gate 22 from "high" to "low". As explained previously, this will cause the output of NAND gate 22 to go from "low" to "high", supplying the necessary signal to turn "off" power gate 20 and turn "on" shorting transistor 21 which will quickly erase the information stored in volatile memory 16. The change in resistance of legs 36 or 37 can be due either to breaks or shorts in either of the legs caused by an attempted intrusion, or by a slow change in resistance of the legs 36 or 37 caused by a chemical attack or by other means. Thus, the circuit shown in Fig. 10 will respond to attempted mechanical or chemical intrusions by sending a signal to the NAND gatc 22 which in turn will send a signal to cause the erasure of information before the intrusion is complete and the volatile memory can be read.

As indicated previously, there are various special attacks whereby screen barriers can be thwarted, compromised, or by-passed without losing data or memory, if extra precautions are not taken. Two such attacks involve controlled exposure to ionizing radiation and, exposure to low temperatures. The circuitry shown in Fig. 11, detects both visible and ionizing radiation and causes the memory 16 to be erased before ionizing radiation is able to permanently affect the volatile memory. The circuit in Fig. 12 detects temperature excursions below a predetermined value and causes the memory to be erased before a critical low temperature affects the volatile memory.

The circuit for Sensor X, which is responsive to both visible and ionizing radiation is shown in Fig. 11. This circuit includes an operational amplifier 62 having one side connected to diode 63 in series with a resistor 64, the combination of which provides a reference voltage to the positive input of the operational amplifier 62. The negative input of the operational amplifier 62 is connected between a photo sensitive device 65, such as a Photo-Darlington pair or a phototransistor, and resistor 66 to system power or battery via power switch 18 and through resistors 67 to ground. Capacitors 68 and 69 and resistors 66 and 70 have been provided for noise filtering. The photosensitive device is located on the card 24 so that it is not blocked by the lead foil sheets 29, preferably adjacent to the volatile memory chip 16 under the notch 30 of the lead foil sheet such that attempted radiation of this component 16 will also expose the photosensitive device 65 to radiation. In normal operation, the photosensitive device 65 is nonconducting in the absence of radiation and the operational amplifier 62 is biased "on". However, when the photosensitive device senses radiation (either ionizing or in the visible spectrum) of sufficient intensity, it will conduct current which will change the bias on the operational amplifier 62 turning it "off". This will cause the NAND gate 22 to turn "on" and provide a signal to power gate 20 and shorting transistor 21 to cause information stored in volatile memory 16 to be erased as previously described.

The circuitry of Sensor T is shown in Fig. 12. In this circuit three resistors 72, 74 and 76, together with resistor 70, provide the four legs of a bridge circuit, which circuit is connected to operational amplifier 78. Resistor 70 is a thermistor having a negative temperature coefficient of resistance, i.e. its resistance increases with decreasing temperature. The value of the three resistors 72, 74 and 76 are chosen to bias operational amplifier 78 normally "on" within the operating temperature range, and to bias the amplifier "off" at a chosen temperature. The value of resistor 76 is chosen based on the temperature characteristics of thermistor 70. Thus in normal operation the operational amplifier 78 is normally biased "on", but when the temperature falls below a selected low value, e.g. 0°C or -20°C or some other value related to the temperature dependent retention characteristics of volatile memory 16, the operational amplifier 78 will turn "off" which as described above, will cause the NAND gate to give a signal which will cause erasure quickly of the information stored in volatile memory 18.

While one embodiment of this invention has been shown and described various adaptations and modifications may be made without departing from the scope of the invention as defined in the appended claims. For example, the NAND gate can be replaced with other logic circuits performing a logical "or" function to cause erasure of the memory if any one of a number of events are sensed indicating that an intrusion is being attempted. Additional sensors could be used to detect other evidence of intrusion.

Claims

1. A barrier for protecting against intrusions into an electronic assembly comprising;
screen means surrounding said electronic assembly, said screen means including line means formed on a substrate in a pattern that resists access without disturbing said line means, said line means being formed of conductive particles of material disposed in a solidified matrix of material, the resistance of said line means charging when said line means are disturbed,
encapsulating material encapsulating said line means and bonded to said line means which bond is stronger than the bond of said line means to said substrate and which encapsulating material is harder and more brittle than said line means, and which encapsulating material is subject to attack by reagents which are similar to reagents which affect said material of said matrix of said line means;
and, electrical supply and signal detection means adapted to supply an input signal to said line means and generate an output signal responsive to a given change in said resistance of said line means;
whereby when said resistance of said line means changes, a signal will be generated.

2. Protecting barrier as defined in Claim 1 wherein the electronic assembly includes volatile memory means, and wherein means responsive to said output signal are provided to erase data contained in said volatile memory means.

3. Protecting barrier as defined in Claim 1 or 2 wherein said line means further comprises a plurality of line segments, and where said electrical supply and detection means detects changes in resistance between two of said line segments.

4. Protecting barrier as defined in Claim 3 wherein said line means form a part of a voltage divider circuit.

5. Protecting barrier as defined in Claim 4 wherein means are provided to generate a signal responsive to the change in resistance of said line segments in said voltage divider circuit.

6. Protecting barrier as defined in Claim 5 wherein said signal is generated by amplifier means connected to said voltage divider circuit.

7. Protecting barrier as defined in anyone of Claims 1 - 6 further characterized by means to detect a temperature excursion below a given temperature value and generate an output signal responsive to the detection of said temperature excursion, and/or by means to detect radiation above a given value and generate said output signal responsive to said detected radiation.

8. Protecting barrier as defined in Claim 7 wherein said means to detect said temperature excursion includes second circuit means having means to provide a reference signal to control response to said temperature excursion.

9. Protecting barrier as defined in Claim 8 wherein said second circuit includes temperature sensitive resistance means which varies its output as a function of temperature, or is a reference bridge circuit.

10. Protecting barrier as defined in Claim 9 wherein said output signal is generated by an amplifier connected in circuit relationship with said second circuit.

11. Protecting barrier as defined in anyone of Claims 1 - 10 further characterized by means to detect radiation intensity above a given value and generate an output signal responsive to said detected radiation.

12. Protecting barrier as defined in Claim 12 wherein said means to detect radiation includes third circuit means having means especially a photosensitive device to vary a characteristic thereof responsive to said detected radiation.

13. Protecting barrier as defined in Claim 12 wherein said third circuit includes an operational amplifier which produces said output signal.

14. Protecting barrier as defined in Claim 11 further characterized by radiation shielding means disposed to reduce radiation received by said volatile memory as compared to radiation received by said means to detect radiation.

15. Protecting barrier as defined in anyone of Claims 2 - 14 wherein gate means are provided to generate said output signal, and/or switch means to turn off the power to said volatile memory responsive to the output signal.

16. Protecting barrier as defined in Claim 15 further characterized by transistor means to short said volatile memory in response to said output signal.

17. Protecting barrier as defined in anyone of Claims 2 - 16 further characterized by means to provide for EMI shielding.

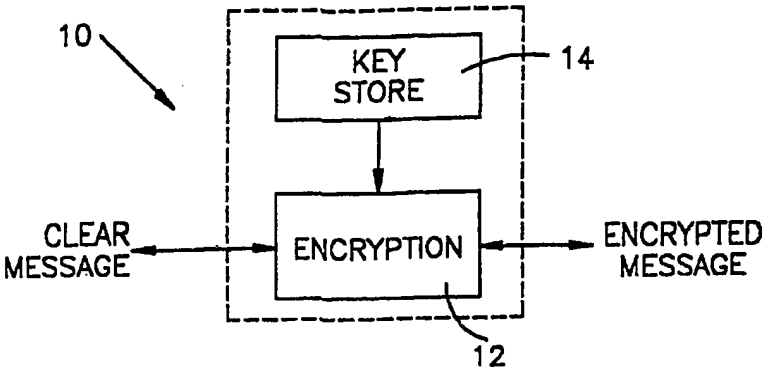
10
KEY STORE
14
CLEAR MESSAGE
ENCRYPTION
ENCRYPTED MESSAGE
12

Fig.1

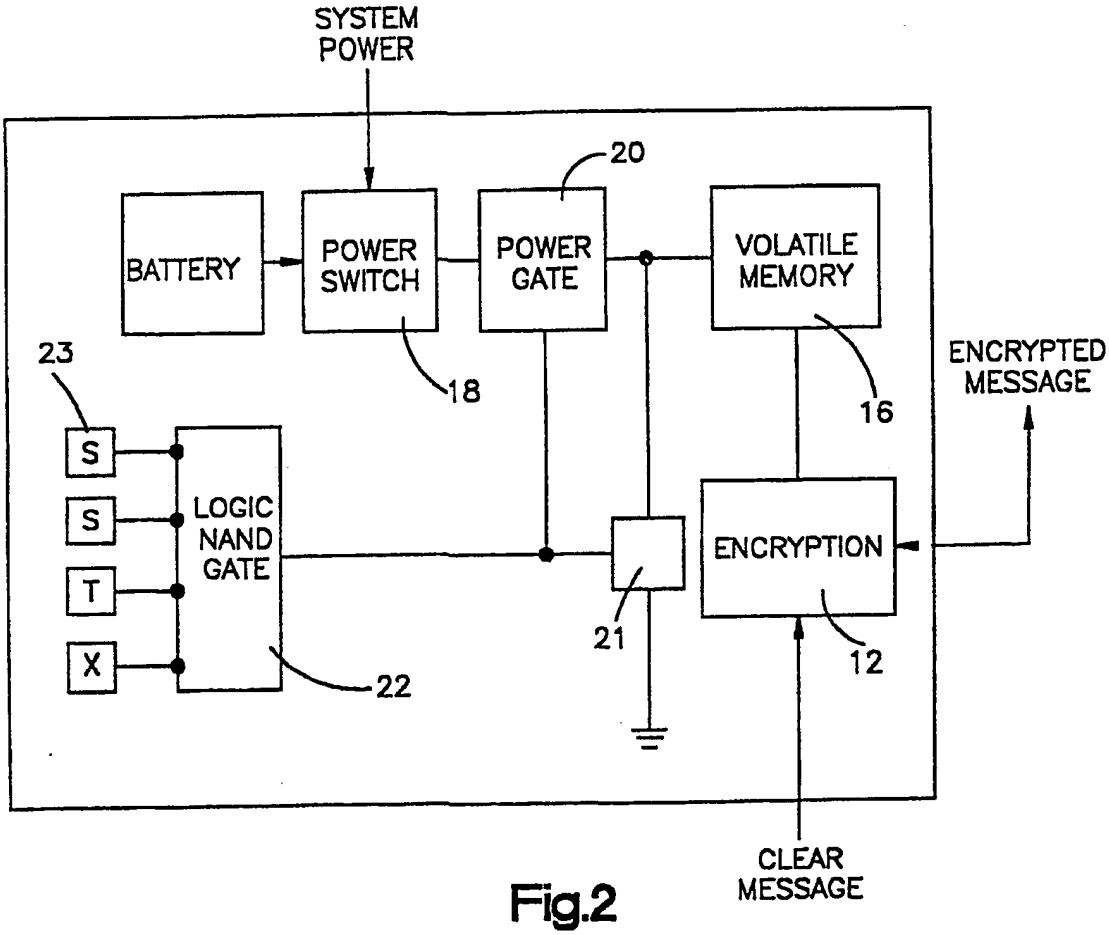
SYSTEM POWER
20
BATTERY
POWER SWITCH
POWER GATE
VOLATILE MEMORY
23
18
16
ENCRYPTED MESSAGE
S
S
T
X
LOGIC NAND GATE
21
ENCRYPTION
12
22
CLEAR MESSAGE

Fig.2

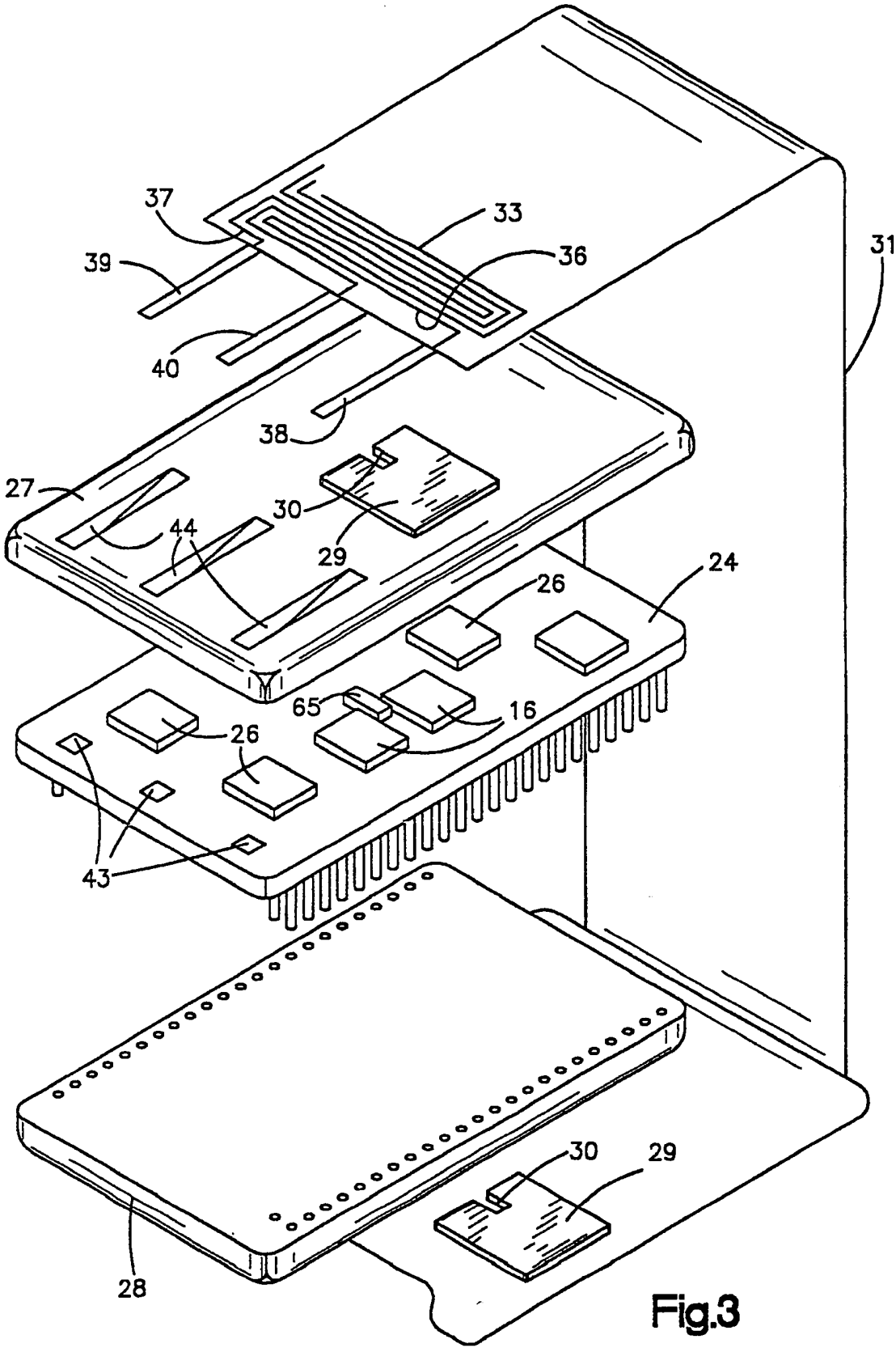

Fig.3

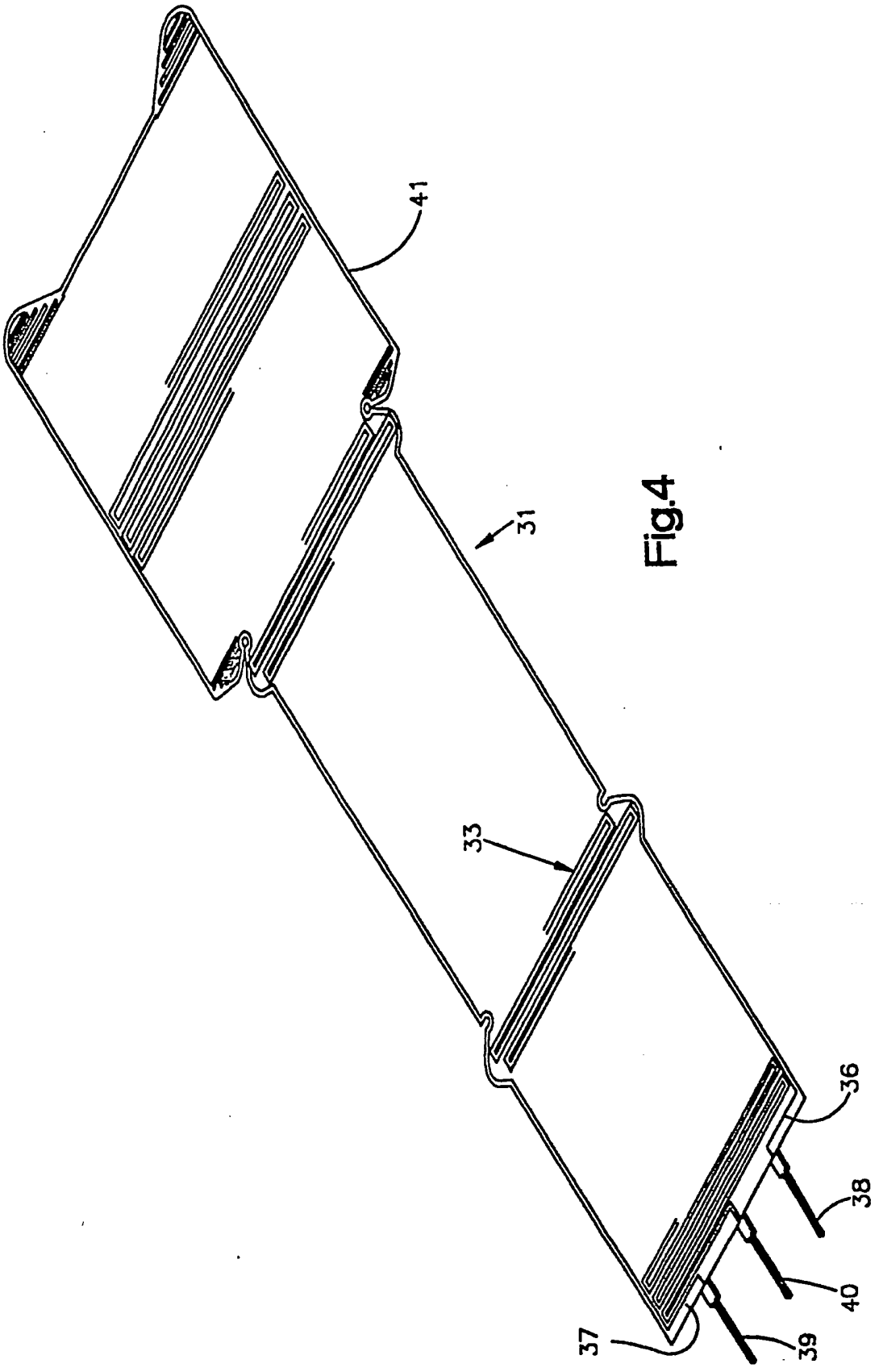

Fig.4

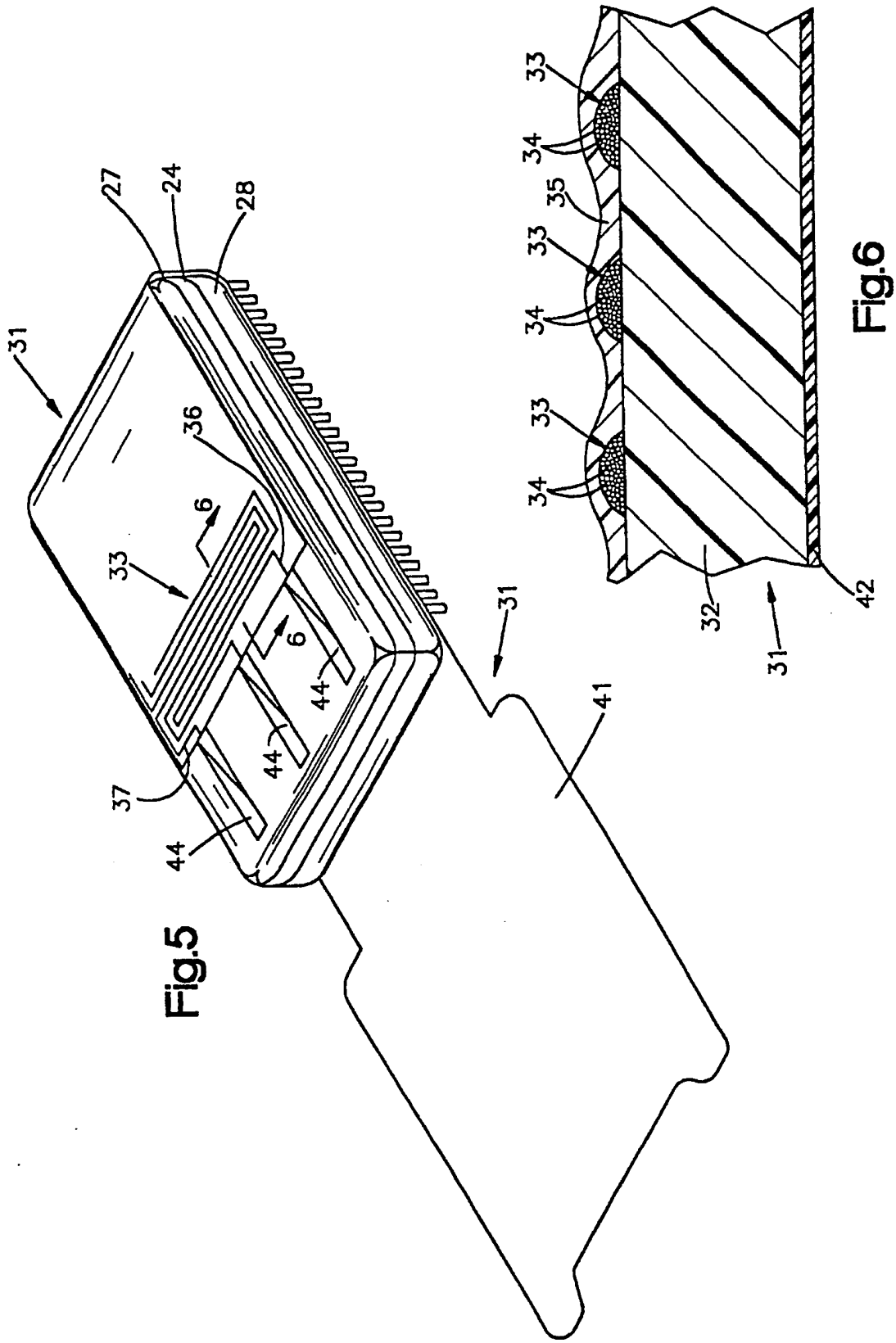

Fig.5

Fig.6

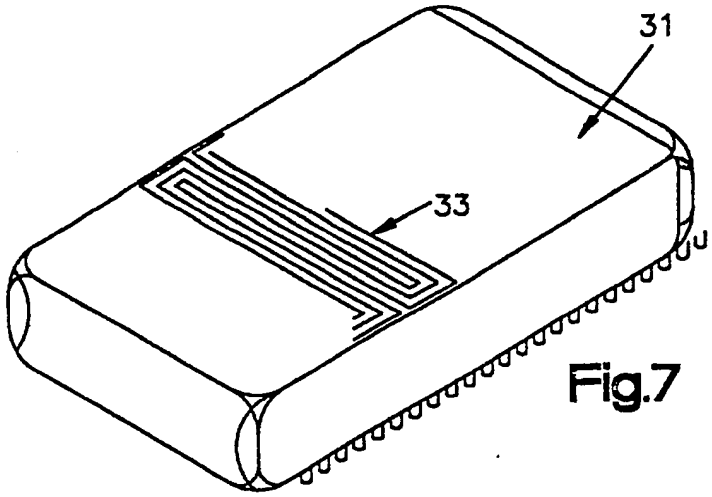

Fig.7

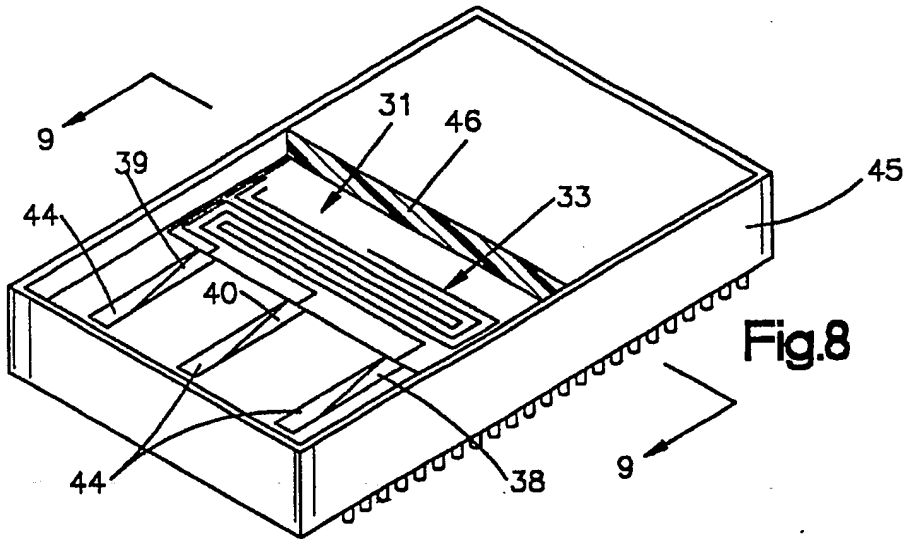

Fig.8

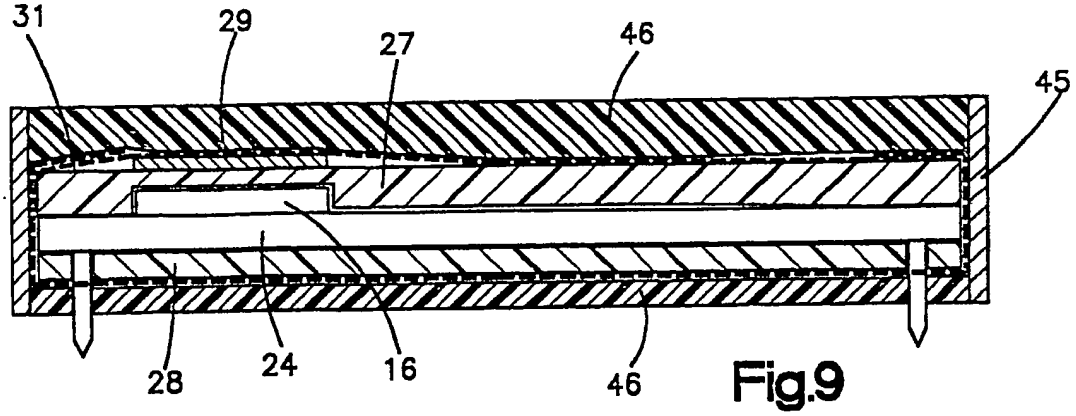

Fig.9

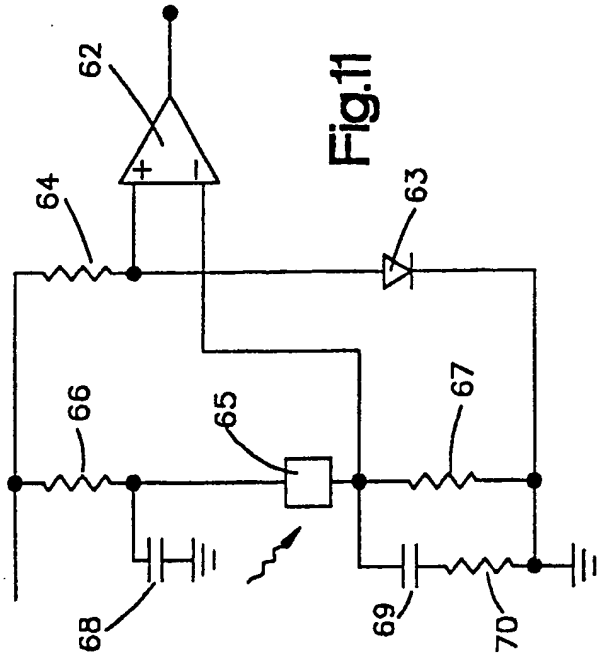

Fig.11

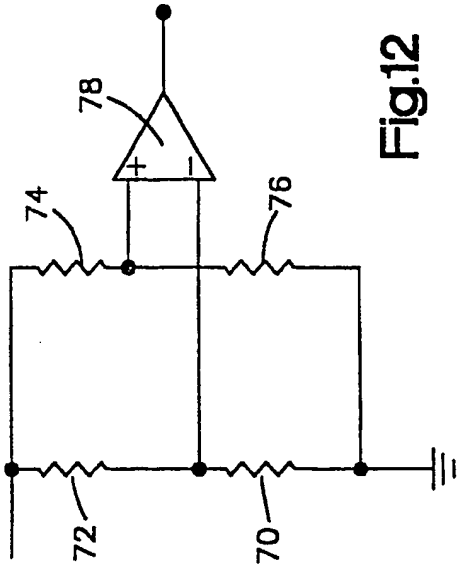

Fig.12

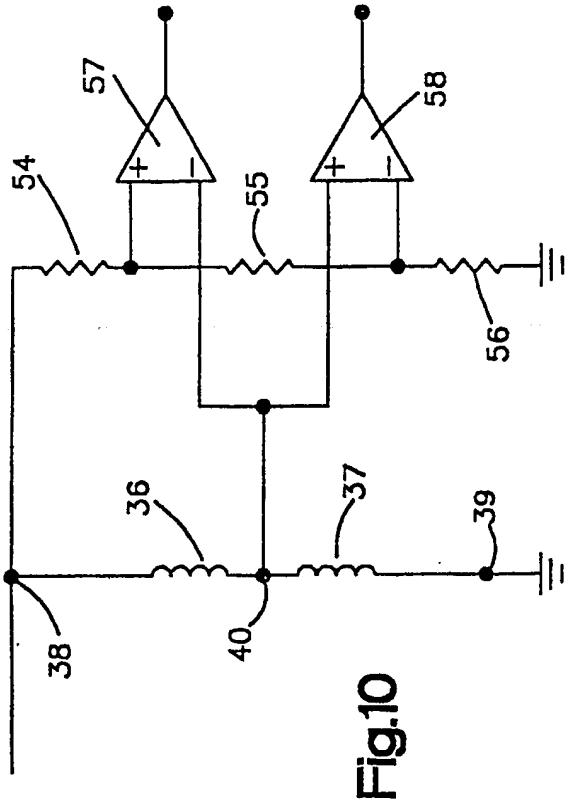

Fig.10